BÜRGERRECHTE

Der gläserne Staatsfeind

Deutsche Unternehmen spielen eine wichtige Rolle auf dem milliardenschweren Markt für Überwachungstechnik, mit der arabische Despoten ihre Bevölkerung ausspionieren. Die Firmen verdienen ihr Geld auch mit Methoden, die in der Bundesrepublik verboten sind.

Er lebt in Bahrain, einem Inselstaat im Persischen Golf, er ist Englischlehrer, verheiratet, Vater eines neunjährigen Sohnes, und außerdem ist er Vorsitzender eines sehr speziellen Vereins, in den nur aufgenommen wird, wer von der Regierung des Landes gefoltert wurde.

Abd al-Ghani al-Chandschar selbst hat dies, wie er sagt, in den vergangenen 17 Jahren sechsmal erdulden müssen, und er hat über diese Erfahrung gesprochen, vor dem britischen Unterhaus und vor Vertretern der Vereinten Nationen.

Seit acht Monaten jedoch ist Chandschar nirgends mehr zu sehen und nicht mehr zu hören. Er ist in Bahrain untergetaucht, Kontakt gibt es nur über Menschenrechtsorganisationen, die das Kürzel kennen, unter dem er mit Hilfe des Internettelefondienstes Skype zu erreichen ist.

Während der ersten Telefonate bleibt der Bildschirm schwarz, nur eine Stimme ist zu hören, die zu einem zurückhaltenden, höflichen Mann gehört. Nachdem er Vertrauen gefasst hat, ist eine kahle Wand zu sehen, links davon ein Fenster, zugezogen mit einem geblümten Vorhang. Chandschar sitzt davor in weißem Hemd, er trägt Kopfhörer und Mikrofon, lächelt entschuldigend und sagt: „Tut mir leid wegen meines Haarschnitts, ich muss das selber machen und habe keinen Spiegel."

Seit über einem halben Jahr lebt Chandschar in diesem Zimmer, er kann fünf Schritte in die eine Richtung gehen, vier in die andere. Er macht das regelmäßig, immer eine Viertelstunde lang, er will fit bleiben, wer weiß, was noch kommt, wer weiß, wofür er seine Kraft noch braucht.

Das Zimmer gehört einem Bekannten, er hat Chandschar hier versteckt, einen Regierungsfeind, der wegen umstürzlerischer Pläne inhaftiert war. Im Februar, der Arabische Frühling hatte begonnen, setzte der König von Bahrain seine Strafe aus, wohl um die Demonstranten in seinem Inselreich zu besänftigen. Chandschar sprach zu den Protestierenden. Wenig später erfuhr er von seiner drohenden Verhaftung, tauchte unter und wurde in Abwesenheit verurteilt, zu 15 Jahren Haft.

Chandschar sagt, es gebe Dutzende Untergetauchte, die sein Schicksal teilen, die mit Folter zum Reden gebracht wurden. Und die im Verhör mit belastendem Ma-

ARNE WEYCHARDT / DER SPIEGEL

Regierungsgegner Chandschar bei Online-Konversation: *Verhaftet, gefoltert, untergetaucht*

GETTY IMAGES

Trovicor-Firmensitz in München: *„Unerwünschte Folgen abwägen"*

terial konfrontiert wurden, mit Abschriften ihrer Telefonate, mit Kopien ihrer E-Mails und ihrer Chat-Beiträge.

Westliche, auch deutsche Überwachungstechnik spielt eine Schlüsselrolle im Machtkampf zwischen arabischen Despoten und ihren aufbegehrenden Untertanen. Die Software aus dem Westen hilft Machthabern, Oppositionelle auszuspionieren und zu verfolgen. Die Hersteller verdienen ihr Geld auf einem Milliardenmarkt, oft mit Methoden, die in Deutschland verboten sind.

Trotzdem sind in der Bundesrepublik rund zwei Dutzend Firmen dieser Branche vertreten, oft handelt es sich um spezialisierte Dienstleister mit Kunstnamen wie Gamma International, Syborg, Utimaco. Sie bleiben lieber unter sich und reagieren auf Anfragen vorzugsweise mit dem Hinweis, man unterliege strikten Verschwiegenheitsklauseln. Die Industrie, die ihren Abnehmern aus Regierungen und Behörden totale Transparenz verspricht, versucht, sich ihr selbst zu entziehen.

Die Käufer digitaler Überwachungstechnik kommen häufig aus undemokratischen Staaten, Libyen, Ägypten, Tunesien, Syrien. Auch in Bahrain, wo eine deutsch-finnische Firma tätig wurde, „Nokia Siemens Networks“. Sie war eine gemeinsame Tochter der beiden Telekommunikationskonzerne Nokia und Siemens und gehört nun einem Investmentfonds, der auf Guernsey, einer Steueroase im Ärmelkanal, registriert ist. Gemanagt wird der Fonds, er heißt Perusa, von zurückhaltenden Kaufleuten in München.

2009 stand Nokia Siemens schon einmal in der Kritik, damals ging es um Iran. Als der Fonds das Unternehmen im selben Jahr übernahm, erhielt es einen neuen Namen, Trovicor.

Für Firmen wie Trovicor hat diese Woche besondere Bedeutung. Denn am Dienstag trifft sich die Branche in Kuala Lumpur bei der Asien-Ausgabe der „ISS World“, einer Fachmesse für technisch versierte Agenten, Ermittler und Polizisten. Sie wird ein Marktplatz sein für Anbieter und Abnehmer, und auch diesmal werden wohl wieder Offizielle aus autoritären Staaten anreisen.

So wie im September in Berlin, bei der „Cyber Warfare Europe“, einem anderen Treffpunkt der Szene. In einem fensterlosen Konferenzraum des Marriott-Hotels führte ein ehemaliger Offizier der Elitetruppe U. S. Marines durchs Programm.

In Berlin war ein neuer, beängstigender Versuch zu besichtigen, totale Überwachung zu schaffen auf Kosten der Freiheit. Und diese Überwachung soll nicht nur zuverlässig funktionieren, sie soll vor allem als exportfähiges Produkt taugen, als leistungsfähiges Werkzeug, das jedem Machthaber in die Hand gegeben wird, der es bezahlen kann, ganz gleich, wen er als Staatsfeind deklariert und wie er ihn behandelt. Die Besucher wirkten angetan. Geboten wurden unter anderem die neuesten Einbruchwerkzeuge, mit denen die Rechner von Verdächtigen zu knacken sind; sogar verschlüsselte Mails und Telefonate, versprechen die Anbieter, müssten für interessierte Dritte kein Geheimnis mehr bleiben.

Einen eigenen Stand auf der Cyber Warfare Europe hatten auch Vertreter der Gamma Group, eines Unternehmenskonglomerats, zu dem zwei Firmen mit Sitz in einem modernen Münchner Bürohaus gehören. Gamma bewirbt sich als führend im Feld der Cyber-Überwachung. Der aktuelle Katalog über das Vorzeigeprodukt „FinFisher“ liest sich wie ein Wunschzettel von Ermittlern – und wie der Alptraum von Bürgerrechtlern. Der Prospekt hat 41 Seiten, er enthält Spionagesoftware für alle möglichen Geräte und Abhörsituationen.

So wirbt Gamma für einen „aktiven Passwort-Schnüffler“, der angeblich sogar geschützte Datenübertragung beim Online-Banking (SSL) knacken und in private, verschlüsselte WLANs eindringen kann. Ein Produkt namens „FinSpy“ soll Live-Überwachung über Webcam und Mikrofon ermöglichen, unbemerkt Dateien herunterladen sowie Skype-Telefonate und -Chats verfolgen können.

In Werbevideos verspricht Gamma den „vollen Zugriff auf die Zielsysteme“, also die Computer und Handys der Spionage-Opfer. Kriminelle sowie echte oder vermeintliche Regimegegner sollen davon natürlich nichts merken. Die Spähprogramme sollen etwa durch „gefälschte Software-Updates“ auf ihren Rechnern landen.

Ahnungslose Nutzer holten sich demnach den Spion auf ihre Geräte, indem sie vermeintlich ihr iTunes-Programm von Apple aktualisierten oder die Software ihres BlackBerrys auf den neuesten Stand brachten. Ist beispielsweise ein BlackBerry einmal infiziert, können die Absender der „FinSpy Mobile“-Spähsoftware nicht nur Gespräche belauschen und SMS mitlesen, sondern auch die im Gerät gespeicherten Kontakte, Fotos, Kalendereinträge und andere Dateien sichten – egal wo auf der Welt das Handy gerade im Einsatz ist. Apple hat die dafür genutzte Sicherheitslücke gerade mit einem echten iTunes-Update geschlossen.

Auf der Berliner Sicherheitskonferenz referierte auch ein schmaler Italiener, Repräsentant der Mailänder Firma „Hacking Team“, einer der Hauptkonkurrenten von Gamma. Er führte im Detail aus, wie verschlüsselte Nachrichten zu knacken seien. Behördenvertreter aus den Vereinigten Arabischen Emiraten, aus Malaysia und Indonesien, allesamt Staaten mit Demokratiedefiziten, hörten interessiert zu.

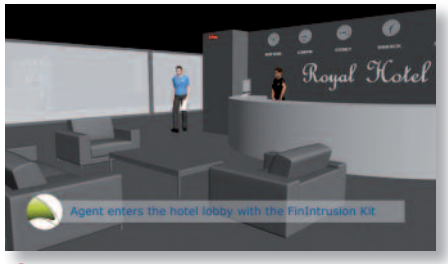
Nicht bei der Verschlüsselung dürfe man ansetzen, die sei auch für einen Supercomputer nicht zu überwinden, erklärte der Italiener; der Schwachpunkt seien die Menschen, die die Geräte nutzen. Stolz führte er daraufhin in einem Video vor, wie perfekt die Überwachung funktioniere, sobald die Spionagesoftware installiert ist. Ein Knopfdruck reiche, schon könnten Ermittler und andere Kunden ein Skype-Gespräch ihrer Zielperson mithören. Oder E-Mails lesen. Oder Kurznachrichten.

Die Software sei bei „einigen tausend Zielpersonen auf fünf Kontinenten im Einsatz“, warb der Mann von Hacking Team. Man habe „hohe Erfolgsraten“ und „viel positives Feedback“. Die Zuhörer applaudierten freundlich.

Abd al-Ghani al-Chandschar erfuhr auf brutale Weise, welche Möglichkeiten die internationale Überwachungsbranche ihren Kunden bietet. In seinem Gefängnis in Bahrain wurde er eines Tages in einen Raum geführt. Dort standen ein Tisch, ein Stuhl. Sie waren fest im Boden verschraubt und standen so dicht beieinan-

Reklame für Spähprogramme

Aus einem Werbevideo für die „FinFisher“-Produktserie der Gamma Group



1 Der Agent loggt sich mit einem Spähprogramm in das Hotel-WLAN ein.

2 Der Agent kommt so an alle Passwörter und Benutzernamen von Anwesenden, die über das Hotel-WLAN ihre E-Mail-Programme oder soziale Netzwerke nutzen.

3 Das Hauptquartier hat fortan Zugang zu allen so erbeuteten Nutzerkonten.

AP

Niederschlagung der Proteste in Bahrain im März: *Wörtliche Mitschriften von Handy-Telefonaten*

der, dass man sich nur mit Mühe setzen konnte. Dann befahl ihm ein Folterknecht aufzustehen, aber das gelang Chandschar nur unvollständig, weil er die Beine nicht durchstrecken konnte. Das ist schmerzhaft, schon nach wenigen Minuten. Und Chandschar durfte sich nicht hinsetzen, er musste stehen. Lange.

Während er stand, fragte ihn sein Folterer nach Feinden des Staates, nach ihren Namen, Adressen.

Chandschar antwortete, er verkehre nicht mit Feinden des Staates.

Kurz darauf hing er unter der Decke, an einem Balken, Handgelenke und Fußknöchel zusammengebunden.

Tage später wurde er erneut aus seiner Zelle zum Verhör geführt und an einen Tisch gesetzt, ihm gegenüber saß ein Mann in Uniform, er hatte ein paar Blatt Papier in der Hand. Es waren wörtliche Mitschriften von Handy-Telefonaten, die Chandschar vor seiner Verhaftung in Bahrain geführt hatte. Seine Folterknechte konnten die Protokolle nur dank der damals eingesetzten westlichen Überwachungstechnik erlangt haben. Bahrain verwendete zum fraglichen Zeitraum, so berichtete die Nachrichtenagentur „Bloomberg“ als Erste, wohl Technik von Nokia Siemens Networks, heute Trovicor.

Immerhin ist Chandschar seinem Schicksal nicht allein ausgeliefert. Wo arabische Behörden und Geheimdienste technisch aufrüsten, sind in wachsender Zahl westliche Aktivisten zur Stelle, um den Oppositionellen beizustehen. Einer von ihnen ist Jacob Appelbaum.

Der Amerikaner beschäftigt sich seit Jahren mit der Überwachungsbranche und dem Kampf gegen Zensur im Netz. Er lebt im Bundesstaat Washington, ist aber viel unterwegs, um Netzaktivisten und Bloggern weltweit dabei zu helfen, im Netz anonym zu bleiben. Appelbaum ist Entwickler beim Tor-Projekt, einer Software, die in Zeiten zunehmender Überwachung anonymes Surfen ermöglichen soll. Dazu werden die Daten verschlüsselt durch verschiedene Computer geschleust, die zum Tor-Netzwerk gehören.

Im Oktober konnte man Appelbaum in Tunis treffen, während einer Konferenz, die von der Heinrich-Böll-Stiftung und einer tunesischen Bürgerrechtsorganisation ausgerichtet wurde. Eingeladen waren vor allem Blogger aus dem arabischen Raum, Appelbaum hielt mit einem befreundeten Hacker einen Vortrag über Privatsphäre und Sicherheit beim Benutzen von Mobiltelefonen. Sein Vortrag lässt sich kurz zusammenfassen: Beides gebe es nicht, sagte Appelbaum; seine Zuhörer blickten unglücklich auf ihre Smartphones.

MARCEL ROSENBACH / DER SPIEGEL

Netzaktivist Appelbaum in Tunis
„Überwachungssysteme sind Waffen“

Appelbaum vergleicht Überwachungsfirmen, die an Despoten liefern, mit Unternehmen im „Dritten Reich“, welche die Nazis mit moderner Technik unterstützten: „Überwachungssysteme sind Waffen, die dazu benutzt werden, Menschenrechtsverletzungen zu begehen“, sagt er. Die Beispiele Ägypten, Syrien und Tunesien machten deutlich, „dass die Geschäfte mit Spähprogrammen aufgedeckt und gestoppt werden müssten“.

Doch die Branche, in der Trovicor, Gamma, Hacking Team und all die anderen agieren, boomt. Der Veranstalter der ISS-Messen, die Firma TeleStrategies, schätzt den Jahresumsatz weltweit auf fünf Milliarden Dollar.

Vielen Anbietern ist es wichtig zu betonen, dass ihre Produkte für legales Abhören und Abschöpfen („lawful interception“) gedacht seien. Beim Sturm auf ein Geheimdienstbüro in Kairo jedoch fiel Aktivisten eine Akte in die Hände, die mit „FinFisher“ beschriftet war. Die Akte enthielt ein detailliertes Angebot für diverse FinFisher-Anwendungen der Gamma Group. Rund 300 000 Euro sollte das System den Unterlagen zufolge kosten. Analysten des ägyptischen Geheimdiens-

tes lobten in anderen Dokumenten besonders die Möglichkeit, Skype-Gespräche abzuhören. Die britische Gamma-Niederlassung bestritt, jemals FinFisher-Produkte nach Ägypten geliefert zu haben.

Die Gamma Group, von der bis Freitagabend keine Stellungnahme zu erhalten war, ist nicht das einzige Unternehmen, das durch die Umbrüche im arabischen Raum in Erklärungsnot kommt. So wurden nach MDR-Recherchen in Libyen Angebotsunterlagen der Firma Syborg aus dem saarländischen Bexbach gefunden. Syborg-Chef Robert Lander erklärt, man gebe wegen Verschwiegenheitspflichten „generell keine Auskunft über Kunden, potentielle Kunden oder Lösungen, die wir anbieten“. Man habe allerdings „bis dato keinerlei Geschäfte mit beziehungsweise in Libyen getätigt“.

Auch in Syrien sollte deutsche Überwachungstechnik offenbar zum Einsatz kommen, als Teil einer Abhöranlage der italienischen Firma Area. Die Italiener verwenden für ihre Systeme seit Jahren Spezialsoftware von Utimaco aus Aachen. Es sei allerdings nur eine Testversion aufgebaut worden, beteuert Utimaco-Chef Malte Pollmann, gerade hätten die Italiener das Projekt ganz eingestellt. „Unsere Software kam nicht zum Einsatz.“

Das glaubte auch das US-Unternehmen Blue Coat sagen zu können, nachdem Internetaktivisten öffentlich gemacht hatten, das Netz in Syrien werde mit Hilfe

„Elektronische Kommunikation ist für staatliche Stellen nirgendwo auf der Welt mehr uneinsehbar.“

von Blue-Coat-Hardware gefiltert und zensiert. Die Firma erklärte zunächst, sie habe nichts an Syrien geliefert. Wenig später musste das Unternehmen kleinlaut einräumen, dass Blue-Coat-Technik im Einsatz war. Es müsse sich um eine Lieferung handeln, so Blue Coat, die für den Irak bestimmt gewesen sei.

Manch ein Branchenvertreter verteidigt derlei offensiv, Jerry Lucas etwa, Veranstalter der ISS-Messen. Gegenüber dem britischen „Guardian“ sagte er, es sei nicht die Aufgabe der Verkäufer, Regierungen in gute und schlechte zu unterteilen: „Wir sind Geschäftsleute, keine Politiker.“

Bei Trovicor heißt es nur, über Kunden und Vertragsinhalte könne man grundsätzlich nicht öffentlich diskutieren. Das übernimmt Christian Hollenberg von Perusa: Es gebe zahlreiche konkrete Belege für die Wirksamkeit von Überwachungstechniken bei der Verhinderung schwerer und schwerster Straftaten. Sei es nicht wünschenswert, dass die Angriffe somalischer Piraten auf deutsche Handelsschiffe effektiver bekämpft werden können? Sei es nicht wünschenswert, dass deutsche Soldaten in Afghanistan besser geschützt werden vor Angriffen von Dschihadisten? Mitarbeiter eines Unternehmens wie Trovicor gingen „auch mit dem Bewusstsein zur Arbeit, an der Verhinderung von Leid mitgewirkt zu haben“, so Hollenberg. Dagegen seien „mögliche unerwünschte Folgen vor allem in halb- oder nichtdemokratischen Ländern abzuwägen“.

Im Übrigen müsse man wissen, „dass elektronische Kommunikation insbesondere für staatliche Stellen heute nirgendwo auf der Welt mehr uneinsehbar ist“. Deshalb müssten Bürger, rät Hollenberg, „in halb- oder nichtdemokratischen Ländern im eigenen Sicherheitsinteresse darauf verzichten, derartige Kommunikationsmittel für Aktivitäten einzusetzen, die sie in Konflikt mit einem herrschenden Regime bringen könnten“.

Es gibt auch Branchenvertreter, die nachdenklich wirken. Utimaco-Manager Pollmann hat nach Bekanntwerden der Syrien-Geschäfte seines Partners Area die Beziehungen mit dieser Firma vorerst eingefroren. Er lässt derzeit für die zurückliegenden 15 Jahre prüfen, bei welchen Kunden Utimaco-Produkte letztendlich gelandet sind. Er habe „verdammt noch mal keinerlei Interesse daran, dass unsere Technik in Syrien eingesetzt wird“. Einen Lieferstopp westlicher Telekommunikationstechnik in den Nahen Osten hält aber auch er „für falsch, weil diese Technologie, wie die Bewegungen dort zeigen, starke freiheitsfördernde Momente beinhaltet“.

Es ist eine verfahrene Situation, im Kern geht es mal wieder um die Frage, was wichtiger ist, Sicherheit oder Freiheit, und wo genau die Grenze gezogen werden soll. Diese Frage ist nicht nur wichtig, wenn es um den Export von Computerprogrammen geht, die als Waffen eingesetzt werden können. Sie ist auch wichtig in Deutschland und höchst umstritten, wie der Einsatz des Staatstrojaners der Firma Digitask durch die Polizei gezeigt hat. Und sie ist nicht einfach zu beantworten, denn beide Seiten haben ihre Argumente, Staatsschützer wie Bürgerrechtler.

Totale Überwachung führt in den Polizeistaat, aber totale Freiheit von Überwachung erschwert es dem Staat, Verbrechen effektiv zu bekämpfen. Bürger verlangen ihre Privatsphäre, Opfer das Überführen der Täter.

In Bahrain nimmt Abd al-Ghani al-Chandschar all diese Aspekte, die erschreckenden technischen Möglichkeiten, die widerstreitenden Argumente, zur Kenntnis. Er sitzt in seinem Zimmer vor der Blumengardine und versucht, sich eine Meinung abzuringen. Er wirkt für einen Moment ratlos. Schließlich sagt er: Er setze auf die Politik, auf die Zivilisierung der Macht, etwas anderes bleibe ihm ja nicht. Uwe Buse, Marcel Rosenbach